UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,410	03/02/2000	Stephen R. Hanna	P4421	5095

207 7590 01/20/2004

WEINGARTEN, SCHURGIN, GAGNEBIN & LEBOVICI LLP
TEN POST OFFICE SQUARE
BOSTON, MA 02109

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 01/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/517,410	HANNA ET AL.	
	Examiner	Art Unit	
	Mossadeq Zia	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/02/2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2,3* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 17 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In claim 17, *the method of claim 17* (page 33, line 28) renders this claim as being indefinite. Appropriate correction is requested.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-7, 13-16, 18, 19, 31-37 are rejected under 35 U.S.C. 102(b) as anticipated by Patent No. 5,748,735, Ganesan.

3. Regarding claim 1, Ganesan discloses a method of operation at a file server comprising:

Accessing at said file server (i) information encrypted with first encryption key (crypto-key) and (ii) an entry from an access control list (Yaksha database), said entry being associated with said encrypted information (Ganesan, col. 9, line 43-46; col. 10, line 38-41) and a client authorized to read and modify said encrypted information, wherein said entry comprises a first decryption key (crypto-key) encrypted with a second encryption key (session key) and wherein

said first decryption key is usable to decrypt said encrypted information (Ganesan, col. 10, line 50-54).

Transmitting to said client said encrypted information and said entry (Ganesan, col. 10, line 48-49, col. 11, line 34-35).

4. Regarding claim 2, Ganesan discloses claim 1 above, further disclose prior to accessing step:

Storing said information encrypted with said first encryption key on said file server (Ganesan, col. 10, line 50-51, 60-63); and

Storing said entry on said file server (Ganesan, col. 10, line 60-61).

5. Regarding claim 3, Ganesan discloses claim 1 above, and further disclose said transmitting step comprises the step of transmitting said encrypted information and said entry in response to a request from said client (Ganesan, col. 10, line 31-33).

6. Regarding claim 4, Ganesan discloses claim 1 above, and further disclose said transmitting step comprises the step of transmitting to said requesting client said access control list (ticket granting ticket from ticket granting server, Ganesan, col. 4, line 40-44, col. 9, 33-34).

7. Regarding claim 5, Ganesan discloses claim 1 above, and further disclose said first encryption key and said first decryption key are symmetric (Ganesan, col. 10, line 43-44).

8. Regarding claim 6, Ganesan discloses claim 1 above, and further disclose said first encryption key comprises one of a public key and a private key of a first public/private key pair and said first decryption key comprises the other of said public key and said private of said first public/private key pair (Ganesan, col. 10, line 44-47).

9. Regarding claim 7, Ganesan discloses claim 2 above, and further disclose said step of storing said entry on said file server includes the step of storing in association with the said entry an unencrypted identifier associated with said client (it is understood by the skilled artisan that a *file name* associated with stored data is an unencrypted identifier and is an inherent feature of a file system that supports the file server, Ganesan, col. 11, line 58-60).

10. Regarding claims 13, 35, 36, 37, Ganesan discloses a method for securely storing information on a file server and distributing the stored information, said method comprising:

encrypting information at one of a plurality of clients in communication with said file server (Ganesan, col. 6, line 5-6, 25), said information being encrypted with a first encryption key (public key) having an associated first decryption key (private key, Ganesan, col. 6, line 6-8);

encrypting said first decryption key with a second encryption key (session key) for each of said plurality of clients authorized to read and modify said information, wherein each respective one of said second encryption keys has a corresponding second decryption key retained by the respective one of said plurality of clients (Ganesan, col. 10, line 26-27);

storing said encrypted information on said file server and storing on said file server said encrypted first decryption keys as a plurality of entries within an access control list (Yaksha database), wherein each one of said entries is associated with one of said plurality of clients (Ganesan, col. 9, line 43-46; col. 10, line 38-41);

forwarding to at least a selected one of said plurality of clients said encrypted information and at least one of said entries (Ganesan, col. 10, line 46-49);

decrypting said encrypted first decryption key contained in said at least one of said entries utilizing the second decryption key corresponding to the second encryption key for the respective entry (Ganesan, col. 10, line 26-28); and

decrypting said encrypted information using said first decryption key to obtain said information (Ganesan, col. 10, line 45-46; col. 11, line 33).

11. Regarding claim 14, Ganesan disclose claim 13 above, and further discloses said forwarding step comprises the step of forwarding said encrypted information (Ganesan, col. 11, line 34-35) and said at least one of said entries to said selected one of said plurality of client: in response to a request received at said file server from said selected one of said plurality of clients (Ganesan, col. 10, line 66-67; col. 11, line 3-4).

12. Regarding claim 15, Ganesan disclose claim 14 above, and further discloses request includes a client identifier (first private key) associated with said selected one of said plurality of clients, said entries each include a client identifier associated with one of said plurality of clients (Ganesan, col. 10, line 66-67), and wherein said forwarding step includes the step of forwarding to at least said selected one of said plurality of clients the said entry including the client identifier associated with the client identifier contained within said request (Ganesan, col. 11, line 10-14).

13. Regarding claim 16, Ganesan disclose claim 13 above, and further discloses forwarding step comprises the step of forwarding to said selected one of said plurality of clients said encrypted information and said access control list (ticket granting ticket from ticket granting server, Ganesan, col. 4, line 40-44, col. 9, 33-34, col. 10, line 52-53).

14. Regarding claim 18, Ganesan disclose claim 13 above, and further discloses first encryption and decryption keys are symmetric (Ganesan, col. 11, line 28-29).

15. Regarding claim 19, Ganesan disclose claim 13 above, and further discloses first encryption key comprises one of a public key and a private key of a first public/private key pair, and the first decryption key comprises the other of said public key and said private key of said first public/private key pair (Ganesan, col. 9, line 40-41).

16. Regarding claim 31, Ganesan disclose a method for accessing information stored securely on a file server

forwarding to said file server a request for information from a client (Ganesan, col. 11, line 20-21);

in response to said, request, receiving from said file server said information encrypted with a first encryption key (user's private key, Ganesan, col. 11, line 16-17) having an associated first decryption key (user's public key, Ganesan, col. 11, line 20-21) and at least one access control list entry associated (Ganesan, col. 9, line 19-20) with a client authorized to read and modify said information (Ganesan, col. 11, line 25-26), said received at least one entry including said first decryption key encrypted with a second encryption key having an associated second decryption key (Ganesan, col. 10, line 6-7);

decrypting said encrypted first decryption key using said second decryption key to obtain said first decryption key (Ganesan, col. 10, line 26-28); and

decrypting said encrypted information using said first decryption key (Ganesan, col. 10, line 45-46; col. 11, line 33).

17. Regarding claim 32, see reasoning to claim 5 stated above.

18. Regarding claims 33, 34, see reasoning to claim 6 stated above.

19. Claim 20 is rejected under **35 U.S.C. 102(b)** as anticipated by Patent No. 5,787,169, Eldridge et al.

20. Regarding claim 20, Eldridge discloses a method for storing information securely on a file server for access by members of a group, said method comprising the steps of:

identifying the members of said group (user quorum) , wherein said group has a group identifier (password key), encrypting information with a first encryption key having an associated first decryption key (Eldridge, col. 2, line 34-37);

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key (Eldridge, col. 2, line 43-47); and

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list (table) associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys (Eldridge, col. 2, line 40-48).

Claim Rejections - 35 USC § 103

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

22. Claims 8-11 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,748,735, Ganesan in view of "Handbook of Applied Cryptography" by Menezes.

23. Regarding claim 8, Ganesan discloses claim 2 above, and further disclose said step of storing said entry on said file server comprising the step of storing an access control list, wherein said entry comprises one entry of a plurality of entries within said access control list, and said entry includes said first decryption key (Ganesan, col. 10, line 39-41) wherein said data stream is encrypted with a second encryption key associated with said client (Ganesan, col. 10, line 50-52); and

said transmitting step comprises the step of transmitting to said requesting client said encrypted information and said access control list key (ticket granting ticket from ticket granting server, Ganesan, col. 4, line 40-44, col. 9, 33-34, col. 10, line 52-53),

but fail to show that said entry includes said first decryption key combined with a check value to form a data stream.

Menezes teach Message Authentication Codes, MAC, (check value) where the originator of a message x (first decryption key) computes a MAC $h_k(x)$ over the message using a secret MAC key k shared with the intended recipient and send both (effectively $x \parallel h_k(x)$) (Menezes, page 364, paragraph 9.6.3, line 3-4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan as per teaching of Menezes to include a MAC to gain the benefit of data integrity on the stream (page 364, paragraph 9.6.3 title).

24. Regarding claim 9, Ganesan and Menezes disclose claim 8 above and further disclose check value (secret MAC key) comprises a value known to said client (Menezes, page 364, paragraph 9.6.3, line 3).

25. Regarding claim 10, Ganesan and Menezes disclose claim 8 above and further disclose said check comprises an identifier (asymmetric crypto-key) associated with said client (Menezes, page 364, paragraph 9.6.3, line 3, Ganesan, col. 9, line 40).

26. Regarding claim 11, Ganesan and Menezes disclose claim 10 above, and further disclose identifier comprises a client identifier that serves to identify said client (Ganesan, col. 9, line 18-19).

27. Claim 12 is rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,748,735, Ganesan in view of "Handbook of Applied Cryptography" by Menezes in further view of Patent No. 5,787,175, Carter.

28. Regarding claim 12, Ganesan and Menezes disclose claim 8 above but fail to show identifier comprises a group identifier that identifies a group of said client is a member.

Carter teach users who are currently members of a collaborative group can readily information (Carter, col. 6, line 12-13). Structures in the prefix portion support collaborative signatures such that members of the group can digitally sign a particular version of the data (Carter, col. 6, line 16-18). An important aspect of these prefix structures is their use of public–key cryptographic (group identifier) methods (Carter, col. 6, line 25-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan and Menezes as per teaching of Carter to include collaborative access control to gain the benefit to prevent unauthorized access by users whose access right have been revoked (Carter, col. 6, line 38-39).

29. Claims 21-30 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,787,169, Eldridge et al. in view of Patent No. 5,748,735, Ganesan.

30. Regarding claim 21. Eldridge discloses a method for accessing information securely stored on a file server for access by members of a group, said method comprising:

identifying the members of said group, wherein said group has a group identifier (Eldridge, col. 2, line 41-42);

encrypting information with a first encryption key having an associated first decryption key (Eldridge, col. 2, line 26-27, 47);

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key (Eldridge, col. 2, line 43-47);

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys (Eldridge, col. 2, line 40-48);

in a first decrypting step, decrypting said encrypted first decryption key with said group decryption key to obtain said first decryption key (Eldridge, col. 2, line 34-37); and

in a second decrypting step, decrypting said encrypted information using said first decryption key to obtain said information (Eldridge, col. 2, line 43-47),

but fail to show that in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said encrypted first decryption key encrypted with said group encryption key;

Ganesan teaches that a system where a symmetric crypto-key (first decryption key) is

encrypted by the security server with a second private key (group encryption key) portion of the file server's crypto-key, to form a encrypted key message. The message is forwarded to the user (Ganesan, col. 6, line 17-20, 22-23).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Eldridge as per teaching of Ganesan to ensure that only the appreciate file server will have access to the symmetric crypto-key (Ganesan, col. 6, line 20-22).

31. Regarding claim 22, Eldridge and Ganesan disclose claim 21 above, and further discloses the step of distributing said group decryption key to said members of said group and said first decrypting step comprises the step of decrypting the encrypted first decryption key by said one of said members of said group using the distributed group decryption key (Ganesan, col. 10, line 5-8).

32. Regarding claim 23, Eldridge and Ganesan disclose claim 21 and further discloses first decrypting step comprises the steps of:

forwarding said encrypted first decryption key to a group server associated with said group identifier (Eldridge, col. 2, line 40-48);

decrypting said encrypted first decryption key at said group server using said group decryption key (Eldridge, col. 2, line 43-47); and

forwarding said first decryption key to said one of said group members (Ganesan, col. 10, line 50-52).

33. Regarding claim 24, Eldridge and Ganesan disclose claim 23 above, and further discloses step of forwarding said first decryption key to said one of said group members comprises the step

of forwarding the first decryption key to said one of said group member over a secure channel (Ganesan, col. 10, line 25-28).

34. Regarding claim 25, Eldridge and Ganesan disclose claim 24 above, and further discloses secure channel is a physically secure channel (Ganesan, col. 8, line 16-21).

35. Regarding claim 26, Eldridge and Ganesan disclose claim 24 above, and further discloses secure channel comprises a non-secure communications path and said step of forwarding the first decryption key to said one of said group members over a secure channel comprises the steps of:

encrypting said first decryption key with a third encryption key having an associated third decryption key known to said one of said group members (Ganesan, col. 10, line 25-28);

forwarding to said one of said group members said encrypted first decryption key encrypted with said third encryption key (Eldridge, col. 2, line 40-48); and

decrypting by said one of said group members, said encrypted first decrypted key encrypted with said third encryption key using said third decryption key (Ganesan, col. 10, line 27).

36. Regarding claim 27, 30, Eldridge and Ganesan disclose claim 26 above, and further discloses the third encryption key comprises a public key of a member public/private key pair and wherein said third decryption key comprises the member private key of said member public/private key pair (Ganesan, col. 8, line 15-16; col. 9, line 67; col. 10, line 1-2).

37. Regarding claim 28, 29, Eldridge and Ganesan disclose claim 26 above, and further discloses third encryption and decryption keys are symmetric (Ganesan, col. 9, line 60-62).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

mz
1/12/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100